ORRISH FINANCE PRIVATE LIMITED

RBI REGISTERED NBFC

REGISTRATION NO. B-03.00208

KNOW YOUR CUSTOMER (KYC) AND ANTI-MONEY LAUNDERING (AML) POLICY

SUMMARY OF THE POLICY

Policy Name	Know Your Customer and Anti Money Laundering Policy
Issue and Effective date	1st, April,2024
Date of next review	Within in 12 months from effective date
Periodicity of review	Annually
Owner / Contact	Compliance Department
Approver	Board of Directors
Annexure	• List of KYC documents for different types of customers as Annexure-A • Procedure for obtaining Identification Information as Annexure- B • Indicative list for risk categorization of customers as Annexure-C. • Digital KYC process Annexure-D

TABLE OF CONTENTS

6. **Principal Officer**
7. **Money Laundering and Terrorist Financing Risk Assessment by Regulated Entities**
8. **Identification of Beneficial Ownership**
9. **Record Retention**
10. **Reporting to Central KYC Registry (CKYCR)**
11. **General Provisions**
12. **Annexure A:** List of KYC Documents for Different Types of Customers
13. **Annexure B:** Procedure for Obtaining Identification Information for Undertaking CDD
14. **Annexure C:** Indicative List for Risk Categorization
15. **Annexure D:** Digital KYC Process

GLOSSARY

- **RBI:** Reserve Bank of India
- **CAP:** Customer Acceptance Policy
- **CIP:** Customer Identification Procedures
- **PMLA:** Prevention of Money Laundering Act
- **PEP:** Politically Exposed Person
- **KYC:** Know Your Customer
- **AML:** Anti-Money Laundering
- **OFPL:** ORRISH FINANCE PRIVATE LIMITED
- **NBFC:** Non-Banking Financial Companies
- **CTR:** Cash Transaction Report
- **STR:** Suspicious Transaction Report
- **FIU – IND:** Financial Intelligence Unit – India
- **CIBIL:** Credit Information Bureau (India) Limited
- **UIDAI:** Unique Identification Authority of India
- **OVD:** Officially Valid Document
- **CERSAI:** Central Registry of Securitization Asset Reconstruction and Security Interest
- **CDD:** Customer Due Diligence
- **NRI:** Non Resident Indian
- **PIO:** Person of Indian Origin
- **V-CIP:** Video-based Customer Identification Process
- **LE:** Legal Entity
- **UCIN:** Unique Customer Identification Number

---

1. INTRODUCTION

ORRISH FINANCE PRIVATE LIMITED (referred to as “the Company” or “OFPL”) is a Non-Deposit Taking Non-Systematically Important NBFC classified as Base Layer NBFC as per Scale Base Regulation registered with the Reserve Bank of India (“RBI”). The company aims to

cater to the needs of individuals, MSMEs, entrepreneurs, companies, and other bodies corporate.

The master direction on Know Your Customer (KYC) issued by the RBI (notification no. DBR.AML.BC.No.81/14.01.001/2015-16 dated February 25, 2016, including amendments dated January 4, 2024) requires all Non-Banking Financial Companies to implement a proper KYC and Anti-Money Laundering (AML) policy, approved by the Board of Directors.

In compliance with the above, the Board of Directors of OFPL has adopted this policy on KYC/AML norms.

2. PURPOSE

This Policy aims to establish and adopt measures and procedures related to KYC, AML, and CFT for the Company in accordance with RBI requirements.

The KYC policy has been framed for the following purposes:

1. To prevent criminal elements from using the company for money laundering and terrorist funding activities.
2. To implement an effective system for customer identification and verification.
3. To enhance understanding of customer financial dealings, facilitating prudent risk management.
4. To establish controls for the detection and reporting of suspicious activities under the AML Act.
5. To ensure compliance with applicable laws and regulatory guidelines.

3. APPLICABILITY

This policy shall prevail over any other document/process/circular/letter/instruction regarding KYC-AML. It applies to all verticals/products of the Company, both existing and future.

The RBI may advise additional measures for managing ML/TF risks.

3. KEY DEFINITIONS

a) "Aadhaar number" shall have the meaning assigned to it in clause (a) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

b) "Act" and "Rules" means the Prevention of Money-Laundering Act, 2002 and the Prevention of Money-Laundering (Maintenance of Records) Rules, 2005, respectively and amendments thereto.

c) "Authentication", in the context of Aadhaar authentication, means the process as defined under sub-section (c) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016.

d) "Board" means Board of Directors of the Company.

e) "Central KYC Records Registry" (CKYCR) means an entity defined under Rule 2(1)(aa) of the Prevention of Money Laundering Rules, to receive, store, safeguard and retrieve the KYC records in digital form of a customer.

f) "Certified Copy" means a comparative copy of the proof of possession of Aadhaar number where offline verification cannot be carried out or officially valid document so produced by the customer with the original and recording the same on the copy by the authorised officer of the company as per the provisions contained in the Act.

g) "Company" means ORRISH FINANCE PRIVATE LIMITED.

h) "Customer" means a person who is engaged in a financial transaction or activity with a company and includes a person on whose behalf the person who is engaged in the transaction or activity, is acting.

i) "Customer Due Diligence (CDD)" means identifying and verifying the customer and the beneficial owner.

j) "Designated Director" means Managing Director or a whole-time Director, or any director duly authorised by the Board of Directors of the Company to ensure overall compliance with the obligations imposed under chapter IV of the Prevention of Money Laundering Act and the Rules;
Explanation:

1. For the purpose of this clause, the terms "Managing Director" and "Whole-time Director" shall have the meaning assigned to them in the Companies Act, 2013.
2. **"Directors"** means individual Directors or Directors on the Board of the Company.

k) "Digital KYC" means the capturing live photo of the customer and officially valid document or the proof of possession of Aadhaar, where offline verification cannot be carried out, along with the latitude and longitude of the location where such live photo is being taken by an authorised officer of the RE as per the provisions contained in the Act.

l) "Digital Signature" shall have the same meaning as assigned to it in clause (p) of subsection (1) of Section (2) of the Information Technology Act, 2000.

m) "Equivalent e-document" means an electronic equivalent of a document, issued by the issuing authority of such document with its valid digital signature including documents issued to the digital locker account of the customer as per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016.

n) "Group" - The term **"group"** shall have the same meaning assigned to it in clause (e) of sub-section (9) of section 286 of the Income-tax Act, 1961 (43 of 1961).

o) "Know Your Client (KYC) Identifier" means the unique number or code assigned to a customer by the Central KYC Records Registry.

p) "KYC Templates" means templates prepared to facilitate collating and reporting the KYC data to the CKYCR, for individuals and legal entities.

q) "Non-face-to-face Customers" mean customers who open accounts without visiting the branch/offices of the Company or meeting the officials of the Company.

r) "Non-Profit Organisations" (NPO) means any entity or organization, constituted for religious or charitable purposes referred to in clause (15) of section 2 of the Income-tax Act, 1961 (43 of 1961), that is registered as a trust or a society under the Societies Registration Act, 1860 or any similar State legislation or a Company registered under Section 25 of the Companies Act, 1956 or applicable Section 8 of Companies Act, 2013.

s) "Officially Valid Document" (OVD) means Passport, Driving license, Proof of possession of Aadhaar Number, Voter's Identity Card issued by the Election Commission of India, Job card issued by NREGA duly signed by an officer of the State Government and letter issued by the National Population Register containing details of name and address.
"*Provided also that where the client submits his proof of possession of Aadhaar number as an officially valid document, he may submit it in such form as are issued by the Unique Identification Authority of India.*"
Explanation:
For the purpose of this clause, a document shall be deemed to be an OVD even if there is a change in the name subsequent to its issuance provided it is supported by a marriage certificate issued by the State Government or Gazette notification, indicating such a change of name.

t) "Offline verification" shall have the same meaning as assigned to it in clause (pa) of section 2 of the Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016 (18 of 2016).

u) "Person" includes an individual, a Hindu undivided family, a Company, a firm, an association of persons, a body of individuals, whether incorporated or not, or every artificial juridical person, not falling within any one of the above persons any agency, office or branch owned or controlled by any of the above persons.

v) "Periodic Updation" means steps taken to ensure that documents, data, or information collected under the CDD process are kept up-to-date and relevant by undertaking reviews of existing records at the periodicity prescribed by the Reserve Bank or act or rules.

w) "Principal Officer" means an officer at the management level nominated by the Company, responsible for furnishing information as per Rule 8 of the Rules.

x) "Politically Exposed Persons" ("PEP") means Persons who are or have been entrusted with prominent public functions in India or foreign country, e.g., Heads of States or of Governments, senior politicians (e.g., MPs, MLAs, MLC, Municipal Counsellors, Panchayat President, Members), senior government/judicial/military officers, senior executives of state-owned corporations, all political party officials, Political Parties, etc.

y) "Regulated Entities" (REs) means all Scheduled Commercial Banks (SCBs)/ Regional Rural Banks (RRBs)/ Local Area Banks (LABs)/ All Primary (Urban) Co-operative Banks (UCBs)/ State and Central Cooperative Banks (St CBs / CCBs) and any other entity which has been licensed under Section 22 of Banking Regulation Act, 1949, which as a group shall be referred as 'banks' All India Financial Institutions (AIFIs) All Non-Banking Finance Companies (NBFCs), Miscellaneous Non-Banking Companies (MNBCs) and Residuary Non-Banking Companies (RNBCs). All Payment System Providers (PSPs)/ System Participants (SPs) and Prepaid Payment Instrument Issuers (PPI Issuers) All authorized persons (APs) including those who are agents of Money Transfer Service Scheme (MTSS), regulated by the Regulator.

z) "Suspicious Transaction" means a "transaction", including an attempted transaction, whether or not made in cash, which, to a person acting in good faith: gives rise to a reasonable ground of suspicion that it may involve proceeds of an offense specified in the Schedule to the Act, regardless of the value involved; or appears to be made in circumstances of unusual or unjustified complexity, or appears to not have an economic rationale or bonafide purpose, or gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
Explanation: Transaction involving financing of the activities relating to terrorism includes transactions involving funds suspected to be linked or related to, or to be used for terrorism, terrorist acts or by a terrorist, terrorist organization or those who finance or are attempting to finance terrorism.

aa) "Transaction" means a purchase, sale, loan, pledge, gift, transfer, delivery or the arrangement thereof and includes:
i. Opening of an account, or
ii. Deposit, withdrawal, exchange, or transfer of funds in whatever currency, whether in cash or by cheque, payment order or other instruments or by electronic or other non-physical means; or
iii. The use of a safety deposit box or any other form of safe deposit; or
iv. Entering into any fiduciary relationship; or
v. Any payment made or received, in whole or in part, for any contractual or other legal obligation; or
vi. Establishing or creating a legal person or legal arrangement.

bb) "Video-based Customer Identification Process (V-CIP)" means a method of customer identification by an official of the company by undertaking seamless, secure, real-time, consent-based audio-visual interaction with the customer to obtain identification information including the documents required for CDD purpose, and to ascertain the veracity of the information submitted by the customer.

cc) "Virtual KYC" means the process of ascertaining the identity of a person using video, images, or any other format of data transmission through electronic means.

All other expressions unless defined herein shall have the same meaning as have been assigned to them under the applicable Master direction on NBFC or the Reserve Bank of India Act, or the Prevention of Money Laundering Act and Prevention of Money Laundering (Maintenance of Records) Rules, any statutory modification or re-enactment thereto or as used in commercial parlance, as the case may be.

4. KEY ELEMENTS

The Company has established its KYC policy, which incorporates the following four key elements:

a) Customer Acceptance Policy
b) Customer Identification Procedures
c) Monitoring of Transactions
d) Risk Management

For the purpose of this KYC policy, a 'Customer' is defined as per Clause 3 (Definitions).

4A. Money Laundering and Terrorist Financing Risk Assessment

a) The Company shall conduct periodic 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessments' to identify, assess, and mitigate risks related to clients, geographic areas, products, services, transactions, and delivery channels. This assessment will consider relevant risk factors to determine the overall risk level and appropriate mitigation strategies. The Company will also take into account sector-specific vulnerabilities communicated by regulators.

b) Risk assessments shall be documented and proportionate to the Company's nature, size, geographical presence, and complexity. The periodicity of these assessments will be determined by the Board or its delegated committee, with a minimum annual review.

c) The outcomes of the risk assessment will be presented to the Board or the relevant committee and made available to competent authorities and self-regulating bodies.

5B. Risk-Based Approach (RBA)

The Company will implement a Risk-Based Approach (RBA) to manage identified risks, supported by Board-approved policies, controls, and procedures. The Company shall adopt a Customer Due Diligence (CDD) program tailored to the ML/TF risks and business size, with ongoing monitoring of these controls.

a) Customer Acceptance Policy (CAP)

The Customer Acceptance Policy will ensure explicit guidelines regarding customer relationships, including:

I. No accounts or loans will be opened or disbursed in anonymous or fictitious names.
II. Loans will not be disbursed if the Company cannot apply appropriate CDD measures due to customer non-cooperation or unreliable documents, which may necessitate filing a Suspicious Transaction Report (STR).
III. All transactions and account-based relationships will require CDD compliance.
IV. Mandatory KYC information will be specified for account opening and periodic updates.
V. Additional information may be obtained with customer consent.
VI. CDD procedures apply at the unique customer identification level, allowing existing compliant customers to avail new loans without fresh CDD.
VII. Risk parameters will be defined based on customer background, activity, location, origin, sources of funds, client profile, and repayment history, facilitating customer categorization (low, medium, high risk).
VIII. Documentation requirements will vary based on customer categories, aligned with the PML Act, 2002 and Reserve Bank guidelines.
IX. Accounts will not be opened or closed without adequate CDD measures, ensuring a high-level decision after due notice to the customer.
X. CDD procedures will apply to all joint account holders, co-applicants, and guarantors.
XI. Clear guidelines will be established for customers acting on behalf of others, adhering to legal standards.
XII. Checks will be conducted to ensure no customer identity matches individuals with criminal backgrounds or banned entities.
XIII. Permanent Account Numbers (PAN) will be verified through the Income Tax verification facility.
XIV. Systems will ensure no customer identity matches sanctioned lists.
XV. Digital signatures of e-documents will be verified as per the Information Technology Act, 2000.
XVI. Goods and Services Tax (GST) details will be verified through the issuing authority.
XVII. The policy will not deny services to financially or socially disadvantaged individuals.
XVIII. If suspicion arises regarding money laundering or terrorist financing, and proceeding with CDD could tip off the customer, the Company will file an STR instead.

The Company's employees will ensure that compliance does not lead to harassment or inconvenience for genuine customers.

b) Customer Identification Procedures

The Company's Customer Identification Procedures (CIP) will be carried out at various stages: during account establishment, financial transactions, or when doubts about previously obtained identification data arise.

Customer identification involves verifying identity using reliable, independent documents, data, or information. Necessary information to establish customer identity includes:

- Satisfactory identification of each new customer, regular or occasional, along with the intended nature of the relationship.
- Compliance with regulatory norms for verifying beneficial owners.
- Enhanced CDD for higher-risk customers.

An indicative list of required documents/information is provided in Annexure-A.

CUSTOMER DUE DILIGENCE PROCEDURES ("CDD")

The true identity and bona fides of customers, whether existing or new, is paramount.

Procedure for Obtaining Identification Information:
CDD will involve obtaining information from individuals, sole proprietorships, partnership firms, and legal entities when establishing account-based relationships. Detailed procedures are attached in Annexure-B.

RISK PROFILING

- The Company will create risk profiles for new customers based on perceived risks.
- Customer profiles will remain confidential and will not be used for cross-selling.
- Enhanced due diligence will apply to higher-risk customers, particularly those with unclear sources of funds.

The risk categorization and the respective profiles are detailed in Annexure-C.

Monitoring of Transactions

Ongoing monitoring is essential for effective KYC procedures. The Company will understand normal customer activity to identify transactions that deviate from this pattern. Key monitoring elements include:

- Special attention to complex or unusually large transactions without apparent lawful purpose.
- Regular reviews of outstanding accounts every six months, focusing on risk categorization and enhanced due diligence needs.
- Maintenance of transaction records as required under the PML Act, 2002, and reporting of suspicious transactions to law enforcement authorities.

PERIODIC UPDATION OF KYC

- Company shall adopt a risk-based approach for periodic updation of KYC ensuring that the information or data collected under CDD is kept up-to-date and relevant, particularly where there is high risk.

S.No.	Basis Risk category	Frequency
1.	High risk customers	Once every two years from the date of opening of the account / last KYC updation
2.	Medium risk customers	Once every eight years from the date of opening of the account / last KYC updation
3.	Low risk customers	Once every ten years from the date of opening of the account / last KYC updation

- The company shall obtain self-declaration from Individual customers and non- Individual customers, through customer registered e mail ID or mobile and registered mobile no, in case of no change in their KYC details. However, in case of change in address of individual customer a self-declaration of such change and proof of new address to be obtained from customer's registered email id, registered mobile no and the declared address shall be verified through positive confirmation within two months, by means such as address verification letter, contact point verification, deliverables etc.
- The Company may obtain a copy of OVD or deemed OVD or the equivalent e-documents thereof, as defined in Section 3(a)(xiii) of Master Direction on KYC, for the purpose of proof of address, declared by the customer at the time of periodic updation.
- Aadhaar OTP based e-KYC in non-face to face mode may be used for periodic updation. To clarify, conditions stipulated in Section 17 are not applicable in case of updation/periodic updation of KYC through Aadhaar OTP based e-KYC in non-face to face mode.
- Declaration of current address, if the current address is different from the address in Aadhaar, shall not require positive confirmation in this case. REs shall ensure that the mobile number for Aadhaar authentication is same as the one available with them in the customer's profile, in order to prevent any fraud.
- In case of change in KYC information of non-individual customer, the Company shall undertake a KYC process which shall be equivalent to on-boarding a new customer.

Enhanced and Simplified Due Diligence Procedure

A. Enhanced Due Diligence

Enhanced Due Diligence (EDD) for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17)

Non-face-to-face onboarding facilitates the REs to establish relationship with the customer without meeting the customer physically or through V-CIP. Such non-face-to-face modes for the purpose of this Section includes use of digital channels such as CKYCR, DigiLocker, equivalent e-document, etc., and non-digital modes such as obtaining copy of OVD certified by additional certifying authorities as allowed for NRIs and PIOs. Following EDD measures shall be

undertaken by company for non-face-to-face customer onboarding (other than customer onboarding in terms of Section 17):

A. In case comapny has introduced the process of V-CIP, the same shall be provided as the first option to the customer for remote onboarding. It is reiterated that processes complying with prescribed standards and procedures for V-CIP shall be treated on par with face-to-face CIP for the purpose of this Master Direction.
B. In order to prevent frauds, alternate mobile numbers shall not be linked post CDD with such accounts for transaction OTP, transaction updates, etc. Transactions shall be permitted only from the mobile number used for account opening. RE shall have a Board approved policy delineating a robust process of due diligence for dealing with requests for change of registered mobile number.
C. Apart from obtaining the current address proof, RE shall verify the current address through positive confirmation before allowing operations in the account. Positive confirmation may be carried out by means such as address verification letter, contact point verification, deliverables, etc.
D. RE shall obtain PAN from the customer and the PAN shall be verified from the verification facility of the issuing authority.
E. First transaction in such accounts shall be a credit from existing KYC-complied bank account of the customer.
F. Such customers shall be categorized as high-risk customers and accounts opened in non-face to face mode shall be subjected to enhanced monitoring until the identity of the customer is verified in face-to-face manner or through V-CIP.

MAINTENANCE OF RECORDS OF TRANSACTIONS AND REPORTING

"Company" has a system of maintaining a proper record of transactions prescribed under Rule 3 of PMLA rules and transaction, procedure, manner of maintaining transactions, and manner of furnishing prescribed under rule 3, 4, 5, 6, 7 and 8 of PML Rules 2005 mentioned below:

A. All cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;
B. All series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;
C. All transactions involving receipts by non-profit organizations of rupees ten lakhs or its equivalent in foreign currency;
D. All suspicious transactions, where forged or counterfeit currency notes or bank notes have been used as genuine and where any forgery of a valuable security has taken place;
E. All suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

The records shall be preserved in the following manner:

i) The nature of transactions
ii) The amount of the transaction and the currency in which it was denominated
iii) The date on which the transaction was conducted
iv) The parties to the transaction

The information in respect of the transactions referred to in clauses I, II and III referred above will be submitted to the Director - FIU every month by the 15th day of the succeeding month.

The information in respect of the transactions referred to in clause IV referred above will be furnished promptly to the Director - FIU in writing, or by fax or by electronic mail not later than seven working days from the date on being satisfied that the transaction is suspicious.

The information in respect of the transactions referred to in clause V referred above will be furnished promptly by the Director - FIU in writing, or by fax or by electronic mail not later than seven working days on being satisfied that transaction is suspicious.

Strict confidentiality will be maintained by the Company and its employees regarding the fact of furnishing/reporting details of such suspicious transactions.

As advised by the FIU-IND, New Delhi; the Company will not be required to submit 'NIL' reports in case there are no Cash / Suspicious Transactions, during a particular period.

The required information will be furnished by the Company directly to the FIU-IND, through the designated Principal Officer.

REPORTING REQUIREMENTS TO FINANCIAL INTELLIGENCE UNIT – INDIA

Company shall furnish to the Director, Financial Intelligence Unit-India (FIU-IND), information referred to in Rule 3 of the PML (Maintenance of Records) Rules, 2005 in terms of Rule 7 thereof.

Explanation: In terms of Third Amendment Rules notified September 22, 2015 regarding amendment to sub rule 3 and 4 of rule 7, Director, FIU-IND shall have powers to issue guidelines to the REs for detecting transactions referred to in various clauses of sub-rule (1) of rule 3, to direct them about the form of furnishing information and to specify the procedure and the manner of furnishing information.

The reporting formats and comprehensive reporting format guide prescribed/ released by FIU-IND and Report Generation Utility and Report Validation Utility developed to assist reporting entities in the preparation of prescribed reports shall be taken note of. The editable electronic utilities to file electronic Cash Transaction Reports (CTR) / Suspicious Transaction Reports (STR) which FIU-IND has placed on its website shall be made use of by REs which are yet to install/adopt suitable technological tools for extracting CTR/STR from their live transaction data.

The Company's Principal Officers, whose all branches are not fully computerised, shall have suitable arrangement to cull out the transaction details from branches which are not yet computerized and to feed the data into an electronic file with the help of the editable electronic utilities of CTR/STR as have been made available by FIU-IND on its website http://fiuindia.gov.in.

While furnishing information to the Director, FIU-IND, delay of each day in not reporting a transaction or delay of each day in rectifying a misrepresented transaction beyond the time limit as specified in the Rule shall be constituted as a separate violation. The Company shall not put any restriction on operations in the accounts where an STR has been filed. The Company shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

However, robust software throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

The Principal Officer can also report information relating to cash and suspicious transactions if detected, to the Director, Financial Intelligence Unit-India (FIU-IND) as advised in terms of the PML rules, 2005 in the prescribed formats at the following address:

Director, FIU-IND,
Financial Intelligence Unit, India,
6th Floor, Hotel Samrat, Chanakyapuri,
New Delhi – 110021

A copy of information furnished shall be retained by the Principal Officer for the purposes of official record.

The Company shall keep the fact of furnishing of STR strictly confidential. It shall be ensured that there is no tipping off to the customer at any level.

However, robust software throwing alerts when the transactions are inconsistent with risk categorization and updated profile of the customers shall be put in to use as a part of effective identification and reporting of suspicious transactions.

a) Risk Management

The Board of Directors of "**Company**" has ensured that an effective KYC program is in place and established appropriate procedures, while constantly overseeing its effective implementation. The programme covers proper management oversight, systems and controls, segregation of duties, training and other related matters. Responsibility has been explicitly allocated within the Company to ensure that its policies and procedures are implemented effectively. The Board of the Company has devised procedures for creating Risk Profiles of new

customers and will apply various Anti Money Laundering measures keeping in view the risks involved in a transaction, account or business relationship.

The Company's internal control and compliance functions have an important role in evaluating and ensuring adherence to the KYC policies and procedures. The compliance function will provide an independent evaluation of the Company's policies and procedures, including legal and regulatory requirements.

"**Company**" will ensure that its internal control systems and machinery are staffed adequately with individuals who are well-versed in such policies and procedures or hire the services of a reputed Company engaged in providing quality services in the said field. The Company will specifically check and verify the application of KYC procedures and comment on the lapses observed in this regard. The compliance in this regard will be presented before the Board at quarterly intervals.

The Company will have an ongoing (at regular intervals) employee training program so that members of the staff are adequately trained in KYC procedures. Training requirements will have different focuses for frontline staff, compliance staff and staff dealing with new customers.

For Risk Management, Company will have a risk-based approach that includes the following:

1. Customers shall be categorized as low, medium and high-risk category, based on the assessment and risk perception of the Company.
2. Each customer will be allotted a Unique Customer Identification Number (UCIN) at the time of sanction of loan by the Company.
3. Risk categorisation shall be undertaken based on parameters such as customer's identity, social/financial status, nature of business activity, and information about the clients' business and their location, etc. Provided that other information collected from different categories of customers relating to the perceived risk is non-intrusive and the same is specified in the KYC policy.

5. DESIGNATED DIRECTOR

Company shall appoint 'Designated Director' who will be responsible for overall compliance with the obligation imposed under Chapter IV of the PML Act.

6 PRINCIPAL OFFICER

Company shall appoint 'Principal Officer' who will be responsible for reporting all transactions and sharing of information. He/ She will also be responsible to ensure that proper steps are e taken to fix accountability for serious lapses and intentional contraventions of the KYC guidelines

7. MONEY LAUNDERING AND TERRORIST FINANCING RISK ASSESSMENT

A. The Company shall carry out 'Money Laundering (ML) and Terrorist Financing (TF) Risk Assessment' exercise periodically to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk for clients, countries or geographic areas, products, services, transactions or delivery channels, etc. The assessment process will consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied. While preparing the internal risk assessment, the Company will take cognizance of the overall sector-specific vulnerabilities, if any, that the regulator/supervisor may share with the Company from time to time.
B. The risk assessment exercise by the Company shall be properly documented and be proportionate to the nature, size, geographical presence, complexity of activities/structure, etc. of the Company. Further, the periodicity of risk assessment exercise shall be determined by the Board of the company, in alignment with the outcome of the risk assessment exercise. However, it will be reviewed at least annually.
C. The outcome of the exercise shall be put up to the Board or any committee of the Board to which power in this regard has been delegated and will be available to competent authorities and self-regulating bodies.
D. The Company shall apply a Risk Based Approach (RBA) for mitigation and management of the identified risk and have Board approved policies, controls and procedures in this regard. Further, the company shall monitor the implementation of the controls and enhance them if necessary.
E. The Company shall monitor the implementation of the controls and enhance them if necessary.

8. DUE DILIGENCE OF BUSINESS PARTNERS

The following due diligence must also be performed on prospective Business Partners.

A) Verify Identity:

A. Obtain and file legible copies of corporate formation and registration documents or public company prospectuses and government filings.
B. PAN card of the Directors etc.
C. Wherever possible (in the case of privately owned entities), arrange for a recommendation from legal counsel to the company.
D. Wherever possible (in the case of privately owned entities), obtain from appropriate government entity confirmation of due incorporation and existence of the corporation.
E. Wherever possible (in the case of privately owned entities), Verify the identity of All directors, Shareholders, UBO of body corporate through various online sources.

B) Verify Source of Income:

1. Research for the Company details in available news or business databases and obtain all corporate earnings information available.

The Company shall maintain files on each Business Partner with copies of all data obtained and memorialize in writing all the verification efforts. These files may be maintained electronically and should be accessible quickly when needed.

8. IDENTIFICATION OF BENEFICIAL OWNERSHIP

The Company will determine the beneficial ownership and controlling interest in case of applicants who are not individuals and the KYC of the beneficial owners will be completed. In the case of beneficial owners, Yes/No authentication provided by UIDAI shall suffice.

Applicable	Guidelines	
Where the client is a company	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has a controlling ownership interest or who exercises control through other means	a. Ownership of/entitlement to more than 10 % of shares or capital or profits of the company b. Control shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders agreements or voting agreements
Where the client is a partnership firm or a company	The beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person	Ownership of/entitlement to more than 10% of the capital or profits of the partnership.
Where no natural person is identified under (i) or (ii) above	The beneficial owner is the relevant natural person who holds the position of senior managing official	

There are certain indicative guidelines issued by RBI from time to time for customer identification requirements for matters such as Trust / Nominee or Fiduciary Accounts, Accounts of companies & firms, Client Accounts opened by professional intermediaries, Accounts of Politically Exposed Persons resident outside India and Accounts of non-face-to-face customers. The Company will adhere to these guidelines to the extent applicable.

9. RECORDS RETENTION

Records pertaining to the identification of the customer and their address obtained while opening their account and during the course of the business relationship will be preserved in accordance with the Section 12 of the PLM Act, 2002. The provision specifies for retention of

records for a period of at least five years after the business relationship has ended in case of all transactions related to the individuals, or for at least five years from the date of the transaction between a client and the reporting entity in case of evidencing identity of its clients and beneficial owners.

10. REPORTING TO CENTRAL KYC REGISTRY (CKYCR)

The customer KYC information will be shared with the CKYCR in the manner mentioned in the RBI Directions in the RBI's KYC templates prepared for 'individuals' and 'Legal Entities (LE)' as the case may be with Central Registry of Securitization Asset Reconstruction and Security Interest of India (CERSAI).

The customer information related to LEs (Legal Entities) will be submitted to CKYCR for accounts of LEs (Legal Entities) opened on or after the commencement of NBFI business activities.

Further, during periodic updation, customers' KYC details will be migrated to current Customer Due Diligence (CDD) standards.

If a customer submits KYC Identifier, with explicit consent to download records from CKYCR, KYC records could be retrieved online from CKYCR and the customer will not be required to submit any KYC records unless in the following events:

A. There is a change in information of customer as existing in the records of CKYCR;
B. The current address of customer needs to be verified;
C. It is considered necessary to verify identity or address of customer, or to perform enhanced due diligence or to build an appropriate risk profile of the client.

KYC Identifier generated by CKYCR will be communicated to the Individual/LE.

11. GENERAL

The Company shall ensure that the provisions of KYC master direction, PMLA and the Rules framed thereunder and the Foreign Contribution and Regulation Act, 1976, wherever applicable, are adhered to strictly. Where the Company is unable to apply appropriate KYC measures due to non-furnishing of information and /or non-cooperation by the customer, the Company may consider closing the account or terminating the business relationship after issuing due notice to the customer explaining the reasons for taking such a decision. Such decisions need to be taken at a reasonably senior level.

ANNEXURE-A

List of KYC Documents for Different Types of Customers

Type of Customer	Type of Proof	Documents
Accounts of individuals	Proof of Identity	I. Copy of Pan Card or II. If a pan card is not available then Form 60
	Proof of address Along with the two latest passport size photographs	(i) Passport (ii) Voter's Identity Card (iii) Driving license (iv) proof of possession of Aadhaar number (iv) Job card issued by NREGA duly signed by an officer of the State Government (v) Identity card (subject to the bank's satisfaction) If above submitted documents does not have updated address then following documents or the equivalent e-documents need to submit: (i) Utility bill (electricity, telephone, post-paid mobile phone, piped gas, water bill); is not more than two months old of any service provider (ii) property or Municipal tax receipt; (iii) pension or family pension payment orders (PPOs) issued to retired employees by Government Departments or Public Sector Undertakings, if they contain the address; (iv) letter of allotment of accommodation from employer issued by State Government or Central Government Departments, statutory or regulatory bodies, public sector undertakings, scheduled commercial banks, financial institutions, and listed companies.
Accounts of Proprietary Concerns		

Name, Address and Activity of the Proprietary Concern.		Proprietor documents: I. Pan card II. Address proof as applicable for an individual account. III. Two latest passport size photographs. Entity documents: I. Proof of the name, address, and activity of the entity, like GST certificate or Shop & establishment license or Any registration/licensing document issued in the name of the proprietary concern by the Central Government or State Government Authority/Department. II. The Company may also accept IEC (Importer Exporter Code) issued to the proprietary concern by the office of DGFT as an identity document for opening of account. III. The complete Income Tax return (not just the acknowledgement) in the name of the sole proprietor where the firm's income is reflected duly authenticated/ acknowledged by the Income Tax Authorities IV. Utility bills such as electricity, water, and landline telephone bills in the name of the proprietary concern.
Accounts of partnership firms		

• Legal name • Address • Names of all partners and their addresses • Telephone numbers of the firm and partners		Documents of partner: I. Pan card of all the partners. II. Address proof as applicable for an individual account. III. The two latest passport size photographs. Partnership firm Documents: I. Permanent Account Number of the partnership firm; II. Proof of the name, address and activity of the entity, like GST certificate or Shop & establishment license or Any registration/licensing document issued in the name of the partnership firm by the Central Government or State Government Authority/Department. III. Partnership deed IV. Authority Letter signed by all the partners. V. The complete Income Tax return of last three years if it is applicable or such lesser period (not just the acknowledgement) in the where the firm's income is reflected duly authenticated/ acknowledged by the Income Tax Authorities. VI. Utility bills such as electricity, water, and landline telephone bills in the name of the partnership firm. VII. Any other prescribed equivalent e-documents.

Accounts of companies		
• Legal name • Address • Names of all partners and their addresses - Telephone numbers of the firm and partners		I. Basic documents of company i.e. Certificate of incorporation, Memorandum & Articles of Association, Permanent Account Number of the company & Any license or registration certificate by central government state government or any regulatory authority of India. II. Resolution by the Board of Directors to obtain a loan from Company and authority to any director or employee to act on behalf of the company. III. One Proof of identity (PAN CARD), Proof of address, and a Colored recent passport size photograph of the authorized person. IV. List of Directors as on date. V. List of Shareholders. VI. Financials statement along with the statutory company's auditor report of the latest preceding completed financial year. VII. Income tax return of last 3 years or such a lesser period as may be applicable along with the Tax audit report. VIII. Any other prescribed equivalent e-documents.

ANNEXURE-B

Procedure for Obtaining Identification Information for Undertaking CDD

The Company shall obtain the following information from an individual while establishing an account-based relationship or while dealing with the individual who is a beneficial owner, authorized signatory or the power of attorney holder related to any legal entity:

a) From an individual who is eligible for enrolment of Aadhaar, the Aadhaar number; the Permanent Account Number (PAN) or the equivalent e-document thereof or Form No. 60 as defined in Income Tax Rules, 1962, as amended from time to time, the proof of possession of Aadhaar number where offline verification can be carried out or not; and such other documents including in respect of the nature of business and financial status of the client, or the equivalent e-documents thereof as may be required by the company.

Provided, where an Aadhaar number has not been assigned to an individual, proof of application of enrolment for Aadhaar shall be obtained wherein the enrolment is not older than 6 months and in case PAN is not submitted, certified copy of an OVD or the equivalent e-document thereof containing details of identity and address and two recent photograph shall be obtained.

Provided that where the customer has submitted:

A. Aadhaar number as mentioned above to the Company, the Company shall carry out authentication of the customer's Aadhaar number using e-KYC authentication facility provided by the Unique Identification Authority of India.
B. Proof of possession of Aadhaar where offline verification can be carried out, the company shall carry out offline verification.
C. Equivalent e-document of any OVD, the company shall verify the digital signature as per the provisions of the Information Technology Act, 2000 (21 of 2000) and any rules issued there under and take a live photo as specified under Annex I of the Master Direction.
D. Proof of possession of Aadhaar number where offline verification cannot be carried out, the company shall carry out verification through an application developed by RE or through his lending service partner or technology partner for this purpose.

"Explanation- Obtaining a certified copy by reporting entity shall mean comparing the copy of officially valid document so produced by the client with the original and recording the same on the copy by the authorised officer of the reporting entity"

Provided further, that from an individual, is not a resident or is a resident in the State of Jammu and Kashmir or Assam or Meghalaya, and does not submit the Permanent Account Number where its client submits his Aadhaar number, ensure such client to redact or blackout his Aadhaar number through appropriate means where the authentication of Aadhaar number is not required under sub-rule (15).

Provided that in case the OVD submitted by a foreign national does not contain the details of address, in such case the documents issued by the Government departments of foreign jurisdictions and letter issued by the Foreign Embassy or Mission in India shall be accepted as proof of address.

Explanation 1: Aadhaar number shall not be sought from individuals who are not 'residents' as defined under these Directions.
Explanation 2: Customers, at their option, shall submit one of the five OVDs.
Explanation 3: Equivalent e-document has also been permitted for accounts of the non-individual customer.

b) In case the identity information relating to the Aadhaar number or Permanent Account Number submitted by the customer does not have a current address, other current address proof defined under Annexure-A shall be obtained from the customer for this purpose. Provided that the client shall submit updated officially valid document with a current address within a period of three months of submitting the above documents."

c) The Company, at the time of receipt of the Aadhaar number, shall carry out, with the explicit consent of the customer, e-KYC authentication (biometric or OTP based) or Yes/No authentication.
Provided:

A. Yes/No authentication shall not be carried out while establishing an account-based relationship.
B. In case of existing accounts where Yes/No authentication is carried out, the Company shall ensure to carry out biometric or OTP based e-KYC authentication within a period of six months after carrying out yes/no authentication.
C. Yes/No authentication in respect of beneficial owners of a legal entity shall suffice in respect of existing accounts or while establishing an account-based relationship.
D. Where OTP based authentication is performed in 'non-face to face' mode for opening new accounts, the limitations as specified in Section 17 shall be applied.
E. Biometric based e-KYC authentication can be done by bank official/business correspondents/business facilitators/ Biometric enabled ATMs.

Explanation 1: While seeking explicit consent of the customer, the consent provisions as specified in Section 5 and 6 of the Aadhaar (Authentication) Regulations, 2016, shall be observed.
Explanation 2: REs shall allow the authentication to be done at any of their branches.

(d) Account may be opened using OTP based e-KYC in non-face to face mode, are also accepted subject to certain conditions.

1. There must be a specific consent from the Customer for authentication through OTP;
2. As regards to borrowal accounts, only term loans shall be sanctioned. The aggregate amount of term loans sanctioned in a year shall not exceed rupees sixty thousand in a financial year;

3. A declaration shall be obtained from the customer to the effect that no other account has been opened nor will be opened using OTP based KYC either with the Company or with any other financial institution.

(e) If the aggregate of borrowal amount of the single borrower, in one or more tranches, is exceeded rupees sixty thousand in a financial year, then the Company shall carry the CDD by using physical mode or Video based Customer Identification Process (V-CIP), as per procedure mentioned in Annexure-1

d) The customer shall submit Permanent Account Number or Form No. 60, , the Permanent Account Number/ form 60 at the time of commencement of an account-based relationship with the Company, the Customer shall submit the same within a period of six months from the date of the commencement of the account based relationship. In case the customer fails to submit Permanent Account Number/Form 60 within the aforesaid six months period, the said account shall cease to be operational till the time Permanent Account Number/ Form 60 is submitted by the customer.

Explanation: In case of asset accounts such as loan accounts, for the purpose of ceasing the operation in the account, only credits shall be allowed.

e) The Company shall duly inform the customer about this provision while opening the account.

f) The customer, shall submit the Permanent Account Number, except one who is a not a resident or resident in the State of Jammu and Kashmir or Assam or Meghalaya, already having an account based relationship with the Company, shall submit his Permanent Account Number or Form No.60, on such date as may be notified by the Central Government, failing which the account shall temporarily cease to be operational till the time the Permanent Account Number or Form No. 60 is submitted by the client:

Provided that before temporarily ceasing operations for an account, the reporting entity shall give the client an accessible notice and a reasonable opportunity to be heard.

Explanation– For the purpose of this clause, “temporary ceasing of operations” in relation an account means the temporary suspension of all transactions or activities in relation to that account by the reporting entity till such time the client complies with the provisions of this clause;

g) If a client has an existing account based relationship with a reporting entity, gives in writing to the reporting entity that he does not want to submit his Permanent Account Number or Form No.60, as the case may be, the client’s account with the reporting entity shall be closed and all obligations due in relation to the account shall be appropriately settled after establishing the identity of the client in the manner as may be determined by the regulator.
Provided that the Company shall serve a notice for the compliance before such date.

h) The Company shall ensure that introduction is not to be sought while opening accounts.

i) Lastly, in case where the individual is a prisoner in a jail, the signature or thumb print shall be affixed in presence of the officer in-charge of the jail and the said officer shall certify the same under his signature. Further, the account shall remain operational only on annual submission of certificate of proof of address issued by the officer in-charge of the jail.

ANNEXURE-C

Indicative List for Risk Categorization

Low-Risk Customers	Medium-Risk Customers	High-Risk Customers
Customers whose identities and sources of wealth can be easily identified and by and large conform to the known customer profile, In such cases, only the basic requirements of verifying the identity and location of the customer are to be met.	• Stock brokerage; • Import/Export; • Gas Station; • Car/Boat/Plane Dealership; • Electronics (wholesale); • Travel Agency; • Telemarketers; • Providers of telecommunications service, internet café, International direct dialling (IDD) call service	• High net worth individuals; • Individuals with dubious reputation as per public information available or commercially available watch lists. • Non-face-to-face customers. • Politically exposed persons (PEPs) or Customers who are close relatives of PEPs. • Individuals specifically identified by regulators, FIU and other competent authorities as high-risk. • Firms with 'sleeping partners'; • Complex business

		ownership structures, which can make it easier to conceal underlying beneficiaries, where there is no legitimate commercial rationale; • Shell companies which have no physical presence in branch locations. The existence simply of a local agent or low-level staff does not constitute physical presence; • Trusts, charities, NGOs/ unregulated clubs and organizations receiving donations

Annexure D

Digital KYC Process

A. The RE shall develop an application for digital KYC process which shall be made available at customer touch points for undertaking KYC of their customers and the KYC process shall be undertaken only through this authenticated application of the REs.
B. The access of the Application shall be controlled by the REs and it should be ensured that the same is not used by unauthorized persons. The Application shall be accessed only through login-id and password or Live OTP or Time OTP controlled mechanism given by REs to its authorized officials.
C. The customer, for the purpose of KYC, shall visit the location of the authorized official of the RE or vice-versa. The original OVD shall be in possession of the customer.
D. The RE must ensure that the Live photograph of the customer is taken by the authorized officer and the same photograph is embedded in the Customer Application Form (CAF). Further, the system Application of the RE shall put a water-mark in readable form having CAF number, GPS coordinates, authorized official's name, unique employee Code (assigned by REs) and Date (DD:MM:YYYY) and time stamp (HH:MM:SS) on the captured live photograph of the customer.
E. The Application of the RE shall have the feature that only live photograph of the customer is captured and no printed or video-graphed photograph of the customer is

captured. The background behind the customer while capturing live photograph should be of white colour and no other person shall come into the frame while capturing the live photograph of the customer.

F. Similarly, the live photograph of the original OVD or proof of possession of Aadhaar where offline verification cannot be carried out (placed horizontally), shall be captured vertically from above and water-marking in readable form as mentioned above shall be done. No skew or tilt in the mobile device shall be there while capturing the live photograph of the original documents.
G. The live photograph of the customer and his original documents shall be captured in proper light so that they are clearly readable and identifiable.
H. Thereafter, all the entries in the CAF shall be filled as per the documents and information furnished by the customer. In those documents where Quick Response (QR) code is available, such details can be auto-populated by scanning the QR code instead of manual filing the details. For example, in case of physical Aadhaar/e-Aadhaar downloaded from UIDAI where QR code is available, the details like name, gender, date of birth and address can be auto-populated by scanning the QR available on Aadhaar/e-Aadhaar.
I. Once the above mentioned process is completed, a One Time Password (OTP) message containing the text that 'Please verify the details filled in form before sharing OTP' shall be sent to customer's own mobile number. Upon successful validation of the OTP, it will be treated as customer signature on CAF. However, if the customer does not have his/her own mobile number, then mobile number of his/her family/relatives/known persons may be used for this purpose and be clearly mentioned in CAF. In any case, the mobile number of authorized officer registered with the RE shall not be used for customer signature. The RE must check that the mobile number used in customer signature shall not be the mobile number of the authorized officer.
J. The authorized officer shall provide a declaration about the capturing of the live photograph of customer and the original document. For this purpose, the authorized official shall be verified with One Time Password (OTP) which will be sent to his mobile number registered with the RE. Upon successful OTP validation, it shall be treated as authorized officer's signature on the declaration. The live photograph of the authorized official shall also be captured in this authorized officer's declaration.
K. Subsequent to all these activities, the Application shall give information about the completion of the process and submission of activation request to activation officer of the RE, and also generate the transaction-id/reference-id number of the process. The authorized officer shall intimate the details regarding transaction-id/reference-id number to customer for future reference.
L. The authorized officer of the RE shall check and verify that:- (i) information available in the picture of document is matching with the information entered by authorized officer in CAF. (ii) live photograph of the customer matches with the photo available in the document.; and (iii) all of the necessary details in CAF including mandatory field are filled properly.;
M. On Successful verification, the CAF shall be digitally signed by authorized officer of the RE who will take a print of CAF, get signatures/thumb-impression of customer at

appropriate place, then scan and upload the same in system. Original hard copy may be returned to the customer.

Banks may use the services of Business Correspondent (BC) for this process.